Práctica 4.

El enunciado de la presente práctica consta de dos documentos:

1. Descripción del ejercicio a realizar
2. Anexo I. Escenario inicial

Objetivo de la práctica

El objetivo de la práctica es proteger el plano de gestión y monitorizar la operación de los dispositivos de red.

La estructura interna de la red corporativa es similar, pero no igual, al de las prácticas anteriores. El escenario que se os proporciona está securizado e incluye una VLAN de Gestión a la que están conectados todos los dispositivos de red y que facilita la realización de esta práctica.

Tareas a realizar:

1. Proteger el acceso a la gestión de los dispositivos de red a través de consola y líneas VTY:

    a. Configura el servidor 172.16.100.100/16 como servidor AAA de tipo RADIUS. Da de alta los dispositivos de red en dicho servidor, utilizando la IP de gestión de los mismos (la perteneciente a la red 172.16.0.0/16) y la palabra clave “conclave”.

    b. La autenticación para el acceso de consola debe realizarse única y exclusivamente contra la base de datos de usuarios local de cada dispositivo.

    c. El acceso remoto debe implementarse únicamente utilizando el protocolo SSHv2 y la autenticación debe realizarse, en primer lugar, contra un servidor de autenticación centralizado AAA de tipo RADIUS y, en caso de fallo, contra la base de datos de usuarios locales.

    d. En cada dispositivo deben crearse dos usuarios:

        i. Usuario: adminlocal – Contraseña: Cisco_123 (este usuario debe acceder directamente al modo privilegiado)

ii. Usuario: userlocal – Contraseña: Cisco_123

e. En el servidor de autenticación AAA, deben crearse dos usuarios:

i. Usuario: admin-remote – Contraseña: Cisco_123
ii. Usuario: user-remote – Contraseña: Cisco_123

f. Debe establecerse la siguiente contraseña para el acceso al modo privilegiado, desde el modo usuario: Clase_123

g. Limita del acceso a la gestión del dispositivo a los host cuya IP esté en la VLAN de gestión.

2. Configura el servidor con la IP 172.16.100.100 como servidor de *syslog*, en el que se volcarán los mensajes de *syslog* de los switches del escenario con un nivel de severidad entre 0 y 5.

3. Se utilizará el servidor con la IP 172.16.100.100 como NMS SNMP. Configura dos comunidades SNMPv2C en Firewall, una de tipo "solo lectura" y otra de tipo "lectura-escritura".

a. Utilizando el *MIB Browser*, obtener el valor del objeto **sysDescr** del grupo **system** de la MIB del agente. Es decir obtener el valor de la instancia del objeto cuyo identificador es `iso.org.dod.internet.mgmt.mib-2.system.sysDescr`.

NOTA: Debido a un problema con algunas versiones de *Packet Tracer 7.1.1* y superiores, los campos *Syntax*, *Access* y *Description* (relativos a las cláusulas SYNTAX, ACCESS, DESCRIPTION incluidas en la definición del objeto) aparecen vacíos. IMPORTANTE: El valor de dichas cláusulas se especifica en la definición del objeto `sysDescr` de la MIB-II incluido en el RFC 1213 (al que el alumno debe acceder vía Web).

b. Utilizando el *MIB Browser,* modifica el valor del objeto `sysName` del grupo `system` de la MIB del agente configurado en *FW*. Comprueba que el valor del nombre del dispositivo ha cambiado realmente.

c. Utilizando el *MIB Browser,* obtén el valor del objeto escalar `ifNumber` y de la tabla `ifTable` del grupo `interfaces` de la MIB del agente configurado en *FW*. Utiliza la operación `Get Bulk` de SNMPv2. El objeto columnar i`fIndex` es el índice de la tabla.

d. Utilizando el *MIB Browser,* deshabilita la interfaz de red GigabitEthernet 0/1 de FW, utilizando la operación `Set`. El objeto columnar o columna `ifAdminStatus` permite activar o desactivar la interfaz administrativamente aplicando los valores 1 (up) y 2 (down). Comprueba el estado de la interfaz.

e. Utilizando el *MIB Browser,* habilita la interfaz de red GigabitEthernet 0/1 de FW, utilizando la operación `Set`. El objeto columnar o columna `ifAdminStatus` permite activar o desactivar la interfaz administrativamente aplicando los valores 1 (up) y 2 (down). Comprueba el estado de la interfaz.

Defensa de la práctica

La defensa de esta práctica se llevará a cabo el 15 de mayo a las 10:00 en la sesión de teoría. El sistema de defensa será similar al utilizado en las defensas de las prácticas anteriores.